Innovative Legal & ICT Counsel

Regolamento UE 679/2016: le principali novità in materia di privacy per le imprese e le pubbliche amministrazioni

Opuscolo informativo

a cura di Gianluca Satta

Fondato e diretto da Massimo Farina

www.diricto.it

info@diricto.it

Il Network raggruppa esperti e studiosi, di tutta l'Italia, in materia di Diritto dell'Informatica e di Informatica Giuridica, con il fine di sviluppare attività di studio, ricerca e approfondimento nell'ambito delle tematiche di interesse comune per il mondo giuridico e informatico.

Edizione: Dicembre 2017

Autore: Gianluca Satta

Il presente lavoro è soggetto a integrazioni e modifiche alla luce dell'evoluzione della riflessione a livello nazionale ed europeo e della normativa in materia.

Sommario

Gianluca Satta

Avvocato del foro di Cagliari, consulente e cultore della materia presso la cattedra di Diritto dell'Informatica e delle Nuove Tecnologie dell'Università degli Studi di Cagliari. Componente del Direttivo del network DirICTo e collaboratore per le attività di ricerca del Laboratorio "ICT4 Law & Forensics" del Dipartimento di Ingegneria Elettrica ed Elettronica dell'Università degli Studi di Cagliari.

Regolamento UE 679/2016: le principali novità in materia di privacy per le imprese e le pubbliche amministrazioni

Introduzione

Il 24 maggio 2016, quattro anni dopo la sua presentazione ufficiale da parte della Commissione Europea, è entrato in vigore il Regolamento (UE) 2016/679.

Il **Regolamento Generale in materia di Protezione dei Dati Personali** (di seguito "Regolamento Generale" o "RGDP") contiene al suo interno l'insieme delle **disposizioni normative in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali** e, insieme alla Direttiva (UE) 2016/680, fa parte del cosiddetto "Pacchetto di protezione dei dati" elaborato ed approvato dall'Unione Europea.

Fino ad oggi, il quadro normativo europeo in materia di protezione dei dati personali era costituito principalmente dalla Direttiva 95/46/CE (cosiddetta "direttiva madre") e dall'insieme degli atti di recepimento di ciascun ordinamento degli Stati Membri. Nel nostro Paese, la Legge 31 dicembre 1996, n. 675 è stato il primo testo normativo adottato in attuazione della direttiva madre, successivamente abrogato e sostituito dal D. Lgs. 30 giugno 2003, n. 196 (Codice della Privacy).

La "direttiva madre" insieme alle disposizioni attuative di ciascun Stato Membro, ha contribuito a creare livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, diversi all'interno di ciascun Stato europeo, ostacolando la libera circolazione dei dati personali all'interno dell'Unione. Inoltre, le divergenze nell'attuazione e nell'applicazione della direttiva 95/46/CE, hanno rappresentato un freno all'esercizio delle attività economiche su scala europea, in grado di falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione.

Per queste ragioni, si è ritenuto necessario intervenire attraverso l'emanazione del Regolamento (UE) 2016/679, in grado di produrre i propri effetti direttamente all'interno degli ordinamenti degli Stati Membri, senza necessità di alcun atto di recepimento.

Il Regolamento Generale in materia di privacy si applicherà a partire dal 25 maggio 2018. L'obiettivo del legislatore europeo, infatti, è quello di garantire a tutti i destinatari delle norme del Regolamento Generale (dagli Stati Membri, ai privati ed alle pubbliche amministrazioni) un tempo di due anni, a partire dalla data di entrata in vigore, per l'adeguamento alle nuove disposizioni normative.

Nei prossimi mesi, quindi, **tutte le imprese e le pubbliche amministrazioni dovranno attivarsi per allineare le proprie attività e i processi interni ai nuovi obblighi previsti dal RGDP entro il 25 maggio 2018.**

Quando si applica il Regolamento privacy?

Riferimenti: art. 2, art. 3 RGDP

Il Regolamento si applica a **tutti i trattamenti di dati personali**, **automatizzati e non**, effettuati da **soggetti** (titolari o responsabili del trattamento) che svolgono le proprie attività **nell'Unione**. Inoltre, il Regolamento trova applicazione anche **nei confronti dei soggetti non stabiliti nell'Unione** che, per offrire beni o fornire servizi o per svolgere attività di monitoraggio di comportamenti, **trattano dati personali di interessati che si trovano nel territorio europeo**.

Sotto un profilo soggettivo, gli obblighi e i principi in materia di privacy si applicano, quindi, sia ai soggetti privati (persone fisiche e/o giuridiche) sia alle autorità pubbliche (pubbliche amministrazioni), i quali possono assumere il ruolo di titolari o di responsabili del trattamento.

Per **trattamento** si intende "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*".

In termini più sintetici, è possibile considerare trattamento ogni operazione che implica un semplice contatto con un dato personale.

L'organizzazione delle figure privacy

Riferimenti: artt. 24, 26, 28 e 29 RGDP

La normativa in materia di protezione dei dati personali, analogamente alla precedente direttiva madre (Direttiva 95/46/CE), prevede una distribuzione dei ruoli e un'organizzazione di tipo gerarchico/piramidale.

Preliminarmente, è opportuno distinguere gli "interessati" dalle altre figure coinvolte; questi, infatti, rappresentano le persone fisiche cui si riferiscono i dati personali oggetto del trattamento.

In cima alla piramide si trova il **titolare del trattamento**, ovverosia il soggetto giuridico a cui spetta decidere le **finalità** e i **mezzi** trattamento. Quasi sempre questa figura corrisponde con il soggetto giuridico (ad esempio, la società o la pubblica amministrazione) che, nello svolgimento di una determinata attività (da cui ne consegue la finalità del trattamento), richiede o necessita di utilizzare i dati personali degli interessati.

Il **responsabile del trattamento** è definito come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*". Si tratta di una figura che opera sulla base di una **delega del titolare**; egli è tenuto a compiere solo le operazioni che il titolare del trattamento ha lui delegato. La figura del responsabile del trattamento è, per questo motivo, **soggetta al potere di controllo del titolare** e per questo si colloca nel gradino più in basso.

Il responsabile del trattamento può essere sia **interno** che **esterno** all'organizzazione del titolare. Nel primo caso, ad esempio, può trattarsi di un dipendente del titolare che svolge mansioni di tipo manageriale o di coordinamento di un'area, al quale sono delegati una parte dei compiti spettanti al titolare del trattamento, per essere eseguiti con riferimento all'area a questi assegnata. Nel secondo caso, invece, il responsabile è esterno quando il titolare del trattamento, necessitando l'acquisizione di un servizio da un fornitore esterno, delega quest'ultimo a svolgere le operazioni di trattamento necessarie per la fornitura del servizio richiesto; tra i casi più frequenti, vi è l'impiego di professionisti esterni per l'espletamento di pratiche di natura fiscale o contabile.

All'ultimo livello della scala gerarchica, si trovano tutti i soggetti che svolgono specifiche **attività di trattamento su autorizzazione del titolare** o **del responsabile del trattamento**. Nella precedente impostazione del Codice della Privacy, questi soggetti erano individuati come "incaricati del trattamento". Nel nuovo Regolamento questa figura, pur non essendo più espressamente prevista, è pienamente compatibile con la struttura e la filosofia del regolamento, in particolare alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza.

Il principio di *accountability* ("responsabilizzazione")

Riferimenti: artt. 5, 23, 25 RGDP

Secondo il principio di responsabilizzazione, il titolare del trattamento ha l'**esclusiva competenza** per il rispetto dei principi e delle regole previste dal Regolamento e, allo stesso tempo, deve essere in grado di **comprovarne** il corretto adempimento.

Tutto l'impianto normativo del Regolamento è basato sul principio di *accountability* di titolari e responsabili. Si tratta di una grande novità in materia di protezione dei dati personali, in quanto ai titolari viene affidato il compito di **decidere autonomamente** le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

Alcune tra le principali espressioni del principio di responsabilizzazione del titolare del trattamento sono:

- Il criterio della "***data protection by design and by default***"
- Il **bilanciamento** fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato
- La **valutazione dei rischi** inerenti il trattamento
- L'adozione di **misure tecniche** e **organizzative** idonee a mitigare tali rischi

In virtù di questa impostazione innovativa, il titolare dovrà adoperarsi per documentare e motivare adeguatamente ogni attività e adempimento, in modo tale da essere sempre

in grado di dimostrare che tali scelte siano coerenti, corrette e pertinenti. Per queste ragioni, la nuova figura del **Responsabile per la protezione dei dati personali** (Data Protection Officer – DPO) costituisce il **fulcro** del processo di attuazione del principio di "responsabilizzazione".

L'informativa e il consenso

Riferimenti: artt. 6, 7, 13, 14 RGDP

Salvo alcuni casi eccezionali, di regola l'informativa e la richiesta di consenso rappresentano due adempimenti fondamentali che ogni titolare deve mettere in atto prima di procedere al trattamento dei dati dell'interessato.

In particolare, affinché il trattamento sia coretto e trasparente è necessario che l'interessato sia **informato dell'esistenza del trattamento e delle sue finalità**. Il titolare del trattamento deve, quindi, fornire all'interessato eventuali ulteriori informazioni necessarie ad assicurare un trattamento corretto e trasparente, prendendo in considerazione le circostanze ed il contesto specifici in cui i dati personali sono trattati

L'informativa è **sempre dovuta** e deve essere fornita nel momento in cui i dati personali sono ottenuti dall'interessato. L'informativa deve essere **concisa**, **trasparente**, **intelligibile** e facilmente **accessibile** e deve essere redatta con un linguaggio **semplice** e **chiaro**, in particolare nel caso di informazioni destinate ai minori.

L'informativa può essere fornita per iscritto o con altri mezzi idonei, anche elettronici. Solo su richiesta dell'interessato, l'informativa può essere data oralmente. Il nuovo Regolamento, inoltre, prevede la possibilità che l'informativa sia fornita attraverso l'utilizzo di icone standardizzate, così realizzando una forma di informativa "stratificata".

Salvo casi particolari, di regola nell'informativa devono essere indicate almeno:

- **l'identità** e i **dati di contatto** del **titolare del trattamento**;
- i **dati di contatto** del **responsabile della protezione dei dati** (DPO);
- le **finalità del trattamento** cui sono destinati i dati personali nonché **la base giuridica del trattamento** (es. disposizione di legge, regolamento, contratto, convenzione, ecc.);
- il **periodo di conservazione** dei dati personali oppure, se non è possibile determinarlo, **i criteri utilizzati** per determinare tale periodo;
- l'esistenza del **diritto dell'interessato** di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- quando il trattamento sia basato sul consenso espresso dall'interessato, l'esistenza del **diritto di revocare il consenso in qualsiasi momento**;
- **il diritto di proporre reclamo** a un'autorità di controllo;
- **l'indicazione** se la **comunicazione** di dati personali rappresenta un **obbligo legale** o **contrattuale** oppure un **requisito necessario** per la conclusione di un contratto, e se

l'interessato ha l'**obbligo di fornire i dati personali** nonché **le possibili conseguenze della mancata comunicazione** di tali dati.

Il **consenso** dell'interessato rappresenta uno dei **fondamenti di liceità del trattamento** previsti dal Regolamento. Il consenso è rappresentato dalla **libera manifestazione della volontà** dell'interessato con cui egli accetta espressamente un determinato trattamento dei propri dati personali, previa informativa da parte del titolare del trattamento. In quanto libera manifestazione di volontà, il consenso può essere **sempre revocato** dall'interessato in qualsiasi momento.

Il consenso, quando è richiesto obbligatoriamente, deve essere sempre **preceduto dall'informativa** e deve riferirsi ad una **specifica** operazione di trattamento; inoltre, non può essere implicito o dedotto da comportamenti dell'interessato.

Quando il trattamento riguarda categorie particolari di dati personali (quali, ad esempio, dati sulla salute, dati biometrici o genetici, dati sulla vita e orientamento sessuale, dati sulle convinzioni religiose o sull'appartenenza sindacale od opinioni politiche) il consenso deve essere anche **esplicito**.

Per il consenso non è prevista la forma scritta, né una forma di documentazione per iscritto. Tuttavia, la forma scritta è l'unica forma idonea a rappresentare l'inequivocabilità del consenso e il suo essere "esplicito". Inoltre, non va dimenticato che il titolare deve essere sempre in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

I diritti dell'interessato

Riferimenti: artt. 12, 15, 16, 17, 18, 21, 22 RGDP

Prima di esaminare nello specifico i singoli diritti, è opportuno tracciare brevemente le regole fondamentali previste dal Regolamento per quanto concerne il rapporto del titolare del trattamento con l'interessato, poste a tutela dei diritti di quest'ultimo. In particolare, il titolare deve sempre comunicare con l'interessato mediante un **linguaggio semplice** e **chiaro**, in forma **concisa**, **trasparente**, **intelligibile**, e garantendo un **facile accesso** alle sue comunicazioni e l'esercizio dei diritti da parte dell'interessato.

Il titolare, ricevuta una richiesta da parte dell'interessato, non può rifiutarsi di soddisfarla e deve fornire le informazioni relative a tutte le azioni da lui intraprese riguarda la richiesta. Il titolare deve garantire la risposta senza ritardo e, in ogni caso, non oltre un mese dal ricevimento della richiesta (salvo l'applicazione del termine di due mesi nei casi previsti dal Regolamento).

Il diritto di accesso

Con l'esercizio di questo diritto, l'interessato ha il **diritto di ottenere dal titolare del trattamento** la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di **ottenere l'accesso ai dati personali** e a tutte le informazioni corrispondenti alle indicazioni obbligatorie dell'informativa (es. finalità del trattamento, categorie di dati personali oggetto del trattamento, eventuali destinatari dei dati, il periodo di conservazione dei dati, e così via). Rispetto al passato, con l'esercizio di questo diritto l'interessato ha **sempre** il diritto di

ricevere **una copia dei dati** personali oggetto di trattamento.

Il diritto di rettifica

Con questo diritto, l'interessato può ottenere dal titolare del trattamento la **rettifica o l'integrazione dei dati personali inesatti o incompleti** che lo riguardano senza ingiustificato ritardo.

Il diritto alla cancellazione ("diritto all'oblio")

In virtù di tale diritto, in presenza di determinate condizioni, l'interessato può ottenere dal titolare del trattamento la **cancellazione dei dati personali** che lo riguardano senza ingiustificato ritardo. A titolo esemplificativo, la cancellazione può essere richiesta quando: i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti; l'interessato revoca il consenso e non sussiste altro fondamento giuridico per il trattamento; l'interessato si oppone al trattamento; i dati personali sono stati trattati illecitamente. La cancellazione, inoltre, può essere richiesta quando i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione (quali, l'offerta di beni e servizi online a distanza).

Il cosiddetto "diritto all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Infatti, è previsto l'obbligo per i titolari, che hanno reso pubblici i dati personali dell'interessato (ad esempio, mediante pubblicazione su un sito web) **di cancellare tali dati e di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati,** compresi qualsiasi link, copia o riproduzione degli stessi.

Il diritto di limitazione di trattamento

Con la limitazione del trattamento, il titolare può esclusivamente conservare il dato e può trattare i dati personali solo con il consenso dell'interessato o per finalità di tutela di un diritto in sede giudiziaria o per motivi di interesse pubblico. Tra i casi previsti dal regolamento, in particolare, la limitazione può essere richiesta quando: l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali; il trattamento è illecito e l'interessato non intende ottenere la cancellazione; il titolare del trattamento non ha più bisogno dei dati personali, ma questi ultimi sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; infine, quando l'interessato si è opposto al trattamento, nell'attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Il diritto di opposizione

Secondo questo diritto, l'interessato può formulare richiesta di opposizione in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. In seguito all'opposizione, il titolare del trattamento **deve astenersi dal trattare i dati personali** salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Qualora i dati personali siano trattati per **finalità di marketing diretto**, l'interessato ha il **diritto di opporsi in**

qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la **profilazione** nella misura in cui sia connessa a tale marketing diretto.

Alla luce delle regole esaminate, al fine di ridurre gli oneri a carico del titolare e per agevolare l'esercizio dei diritti da parte dell'interessato, è opportuno prevedere dei meccanismi, anche automatizzati per richiedere e, se del caso, ottenere gratuitamente, in particolare l'accesso ai dati, la loro rettifica e cancellazione e per esercitare il diritto di opposizione. Tali misure, ad esempio, potrebbero consistere in soluzioni tecnologiche atte a consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali. Con riferimento al diritto di limitazione, invece, potrebbe essere utile prevedere modalità tecniche per "contrassegnare" il dato personale oggetto della limitazione, per il periodo in cui sussiste tale condizione.

Quando l'interessato formula richiesta di rettifica, cancellazione o limitazione, il titolare del trattamento è tenuto a **comunicare l'esercizio di tali diritti a ciascuno dei destinatari cui sono stati trasmessi i dati personali**, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

Infine, oltre ai diritti sin qui illustrati, va evidenziato il diritto dell'interessato a **non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato**, compresa la **profilazione**, che produca **effetti giuridici che lo riguardano** o che incida in modo analogo **significativamente sulla sua persona.**

La portabilità dei dati.

Riferimenti: art. 20 RGDP

Il diritto alla portabilità dei dati consiste nella possibilità per l'interessato di **ricevere i dati personali che lo riguardano** forniti a un titolare del trattamento **in un formato strutturato**, di **uso comune** e **leggibile** da dispositivo automatico e nel diritto di **trasmettere tali dati a un altro titolare del trattamento** senza impedimenti da parte del titolare del trattamento, anche mediante trasmissione diretta quando tecnicamente possibile.

In altri termini, la portabilità dei dati rappresenta una forma di diritto di accesso particolare, potenziata per accrescere il controllo degli interessati sui propri dati. Infatti, l'esercizio di tale diritto consente all'interessato di effettuare facilmente il passaggio da un fornitore di servizi all'altro, garantendo maggiori diritti e un controllo più ampio sui dati personali da parte dell'interessato.

La portabilità può riguardare solo i dati personali riferiti all'interessato e solo quelli che sono stati forniti dallo stesso, e l'esercizio di tale diritto non deve ledere i diritti e le libertà altrui.

Tutti i titolari del trattamento che ricadono nel campo di applicazione di questo diritto, quindi, devono adottare tutte le misure necessarie per consentire all'interessato di ottenere **i dati richiesti in un formato interoperabile**, in modo tale da **consentire ad altri titolari del trattamento di utilizzarli nei propri sistemi.** Inoltre, sarebbe opportuno mettere a disposizione degli interessati idonei strumenti per consentire agli stessi di scegliere i dati che desiderano trasmettere e ricevere escludendo (se del caso) i dati di altri interessati.

Gli adempimenti interni: il registro dei trattamenti.

Riferimenti: art. 30 RGDP

Il registro delle attività di trattamento è un documento scritto, anche in formato elettronico, nel quale sono presenti una serie di informazioni obbligatorie che riguardano le attività di trattamento eseguite dal titolare del trattamento.

L'obbligo di tenuta del registro, previsto a carico di tutti i titolari o responsabili del trattamento, **non si applica** nei confronti delle imprese o organizzazioni che contano **meno di 250 dipendenti**, a condizione che il trattamento effettuato **non presenti alcun rischio** per i **diritti** e le **libertà** dell'interessato, il trattamento sia di carattere **occasionale**, oppure il trattamento non riguarda **categorie particolari di dati** (sensibili), o i dati personali relativi a **condanne penali** e a **reati** il registro è sempre obbligatorio (a prescindere dal numero di dipendenti).

Nel registro devono essere indicati obbligatoriamente: il nome e i **dati di contatto del titolare** del trattamento (ove applicabile, del contitolare, del rappresentante del titolare e del responsabile della protezione dei dati), le **finalità** del trattamento, la descrizione delle **categorie** di **interessati** e delle categorie di **dati personali**, le categorie di **destinatari** a cui i dati personali sono stati o saranno comunicati, eventuali **trasferimenti** di dati personali verso un paese terzo o un'organizzazione internazionale, i **termini** ultimi previsti **per la cancellazione** delle diverse categorie di dati e, infine, una descrizione generale delle **misure di sicurezza tecniche** e **organizzative** adottate a tutela dei dati personali.

Come si può notare, il registro delle attività di trattamento riprende, per contenuto e forma, quello del Documento Programmatico sulla Sicurezza (DPS) già previsto nel Codice della Privacy e poi abrogato a partire dal 2012 e, essendo un documento riepilogativo, come il vecchio DPS, la sua funzione è quella di facilitare la cooperazione tra il titolare/responsabile del trattamento e l'Autorità di controllo.

Le misure di sicurezza.

Riferimenti: art. 32 RGDP

Il titolare del trattamento, a partire dal momento in cui ha in carico i dati personali dell'interessato, ha il **dovere di garantirne la sicurezza**.

Nel Regolamento non sono previste espressamente e tassativamente le misure di sicurezza, come avveniva in passato con l'allegato B del Codice della Privacy (con le cosiddette "misure minime di sicurezza"), bensì sono previsti dei **criteri** e dei **principi** per la **determinazione delle misure di sicurezza**. Come si è detto, in forza del principio di responsabilizzazione dei titolari del trattamento, spetta a questi ultimi mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenuto conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento e del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Da ciò si può agevolmente comprendere come, per una corretta individuazione delle misure di

sicurezza da adottare, sia fondamentale effettuare la **valutazione dei rischi**. Tale attività, necessaria per l'individuazione delle cosiddette "misure idonee di sicurezza" durante la vigenza del vecchio Codice della Privacy, con il Regolamento ha acquisito maggiore importanza e rilevanza in quanto, non essendo più presente la distinzione tra misure minime e misure idonee di sicurezza, rappresenta il **punto di partenza per sviluppare ogni tipo di misura tecnica** e **organizzativa** per garantire la **sicurezza** dei dati personali.

Per una corretta attività valutativa, il titolare dovrebbe innanzitutto individuare quali sono i rischi inerenti alla propria attività di trattamento, quando possono sorgere e gli eventi che costituiscono il fattore di rischio. Una volta effettuata la valutazione dei rischi, sarà possibile individuare le misure tecniche e organizzative adeguate.

A mero titolo esemplificativo, per **misure organizzative** si intende: la formazione del personale, l'adozione di piani di evacuazione, di registri degli accessi in determinati luoghi, l'uso di un sistema di allarme e, infine, l'introduzione di una procedura finalizzata a verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative stesse, anche coinvolgendo altre figure (quali il DPO, l'amministratore di sistema, i responsabili del trattamento interni). Nell'ambito delle **misure tecniche**, invece, si possono individuare: la pseudonimizzazione e la cifratura dei dati personali, l'adozione di un sistema di autenticazione e di autorizzazioni, procedure di *backup*, *data recovery* e continuità operativa, utilizzo di sistemi di protezione informatica (quali *antivirus* e *firewall*) e tutte le altre misure in grado di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.

La valutazione di impatto sulla protezione dei dati personali

Riferimenti: art. 35 RGDP

La valutazione di impatto (o "*Data Protection Impact Assessment*" – DPIA) è un adempimento interno previsto quando il trattamento, in particolare se eseguito mediante l'uso di nuove tecnologie, può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**. La valutazione del rischio, in questo caso, deve essere effettuata tenendo conto di una serie di fattori: la natura, l'oggetto, il contesto e le finalità del trattamento.

Il Regolamento prevede un elenco, sebbene non esaustivo, di casi e condizioni in presenza dei quali è necessario procedere alla valutazione di impatto. In particolare, la DPIA è prevista:

- quando il trattamento comporta una **valutazione sistematica** e **globale** di aspetti personali relativi a persone fisiche, basata su un **trattamento automatizzato**, compresa la **profilazione**, e **sulla quale si fondano decisioni** che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche (ad esempio, trattamento automatizzati volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi).
- quando il **trattamento** riguarda categorie particolari di dati personali ("**sensibili**") o di

dati relativi a condanne penali e a reati (ad esempio, trattamenti di dati genetici, dati biometrici, dati relativi alla salute e alla vita sessuale, trattamenti di dati "**giudiziari**")

- quando il trattamento consente la **sorveglianza sistematica** su larga scala di una **zona accessibile al pubblico** (ad esempio, la videosorveglianza per il controllo sistematico del traffico autostradale).

Per agevolare il lavoro di valutazione, l'Autorità di controllo è incaricata di redigere e rendere pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati e un elenco dei trattamenti per i quali non è previsto tale adempimento.

Nei casi in cui è obbligatoria, la DPIA deve essere effettuata prima di procedere al trattamento dei dati personali da sottoporre alla valutazione. Nel documento contenente la valutazione di impatto è necessario inserire: la **descrizione sistematica dei trattamenti** previsti e delle **finalità** del trattamento, la valutazione della **necessità** e **proporzionalità** dei trattamenti in relazione alle finalità, la **valutazione dei rischi** per i diritti e le libertà degli interessati e, infine, le **misure previste per affrontare i rischi**, includendo le **garanzie**, le misure di **sicurezza** e i **meccanismi** per garantire la protezione dei dati personali e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Quando il titolare non intende procedere alla valutazione di impatto, in virtù del principio di responsabilizzazione, è tenuto a documentare la scelta della mancata conduzione della DPIA, allegando o annotando l'opinione del responsabile della protezione dei dati (DPO) in merito a tale scelta.

Il Responsabile della protezione dei dati personali (DPO)

Riferimenti: artt. 37, 38, 39 RGDP

La figura del Responsabile della protezione dei dati personali (o *Data Protection Officer* - DPO) **non va confusa** con quella del responsabile del trattamento dei dati personali inquadrata nell'organizzazione gerarchico-piramidale.

Il DPO è nominato dal titolare o dal responsabile del trattamento. La sua nomina è obbligatoria quando:

a) il trattamento è effettuato da **un'autorità pubblica** o da un **organismo pubblico**;
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in **trattamenti** che, per loro natura, ambito di applicazione e/o finalità, richiedono il **monitoraggio regolare** e **sistematico** degli interessati **su larga scala**;
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel **trattamento**, su **larga scala**, di **categorie particolari di dati personali:** dati "sensibili" e dati "giudiziari".

Dal punto di vista organizzativo, un gruppo imprenditoriale può nominare un **unico responsabile della protezione dei dati** e, qualora il titolare o il responsabile del trattamento sia **un'autorità pubblica o un organismo pubblico**, può essere designato un **unico responsabile**

della protezione dei dati per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione

Sotto il profilo contrattuale, il DPO può essere un soggetto interno, **dipendente** del titolare o del responsabile del trattamento, oppure può essere nominata una figura esterna all'organizzazione, inquadrata sulla base di un **contratto di servizi**.

Quando il titolare o il responsabile del trattamento **non è tenuto alla nomina del DPO**, ma sceglie di nominare un Responsabile della protezione dei dati personali, deve comunque **osservare tutte le regole previste da Regolamento per la sua nomina**. Per le medesime ragioni, in forza del principio di responsabilizzazione che impone al titolare di adottare misure tecniche ed organizzative per essere in grado di **dimostrare** che il trattamento è svolto conformemente al Regolamento, è sempre opportuno documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire l'applicabilità o meno dell'obbligo di procedere alla nomina del DPO, così da poter dimostrare che nell'analisi sono stati valutati correttamente tutti i fattori pertinenti.

I requisiti del DPO

Il soggetto nominato Responsabile della protezione dei dati deve garantire il rispetto di specifici requisiti. In primo luogo, il DPO deve possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. A tal fine, non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali; tuttavia, la partecipazione a corsi di formazione può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze. In secondo luogo, il DPO deve essere in grado di adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse.

I compiti del DPO

Il Responsabile della protezione dei dati, in particolare, ha il compito di:

- **sorvegliare** l'osservanza del regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
- **collaborare** con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);
- **informare** e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
- **cooperare** con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;
- **supportare** il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento .

Al fine di consentire al DPO di espletare i propri compiti, il titolare del trattamento deve **pubblicare i dati di contatto** (non necessariamente i dati identificativi) **del responsabile della protezione dei dati** e, allo stesso tempo, deve **comunicarli all'autorità di controllo.**

Inoltre, il titolare o il responsabile del trattamento devono mettere a disposizione del Responsabile della protezione dei dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti e assicurarsi che il DPO sia **tempestivamente** e **adeguatamente coinvolto** in tutte le questioni riguardanti la protezione dei dati personali.

La posizione del DPO

La nomina del DPO deve essere effettuata in modo tale da garantire sempre che il soggetto nominato operi in totale indipendenza e, pertanto, **non riceva alcuna istruzione** per quanto riguarda l'esecuzione delle sue funzioni. Inoltre, nel caso in cui al DPO sono attribuiti altri compiti e/o funzioni, il titolare o il responsabile del trattamento devono assicurarsi che tali compiti e funzioni non diano origine ad **un conflitto di interessi**. In linea di principio, ciò significa che non potrà essere designato come DPO un soggetto che si trova in una posizione tale da incidere sulla determinazione delle finalità o sugli strumenti del trattamento di dati personali.

La violazione dei dati personali (*data breach*)

Riferimenti: art. 33 e art. 34 RGDP

Il Regolamento definisce la violazione dei dati personali come "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*". In altri termini, la violazione dei dati personali (cosiddetta "*Data breach*") consiste in **qualunque avvenimento** che mette a **rischio i dati personali** in possesso del titolare del trattamento (ad esempio, un accesso non autorizzato ai dati con conseguente sottrazione di dati, la cancellazione, la sopravvenuta indisponibilità dei dati, e così via).

Quando il titolare del trattamento subisce una violazione dei dati personali e, secondo la sua valutazione, è probabile che sia presente un rischio per i diritti e le libertà delle persone fisiche, procede alla **notifica** della violazione **all'Autorità di controllo**.

La notifica deve essere effettuata dal titolare del trattamento **senza ingiustificato ritardo** (ovverosia, non appena ne ha notizia), comunque **entro 72 ore** dal momento in cui ne è venuto a conoscenza. Se effettuata oltre le 72 ore il titolare dovrà motivarne il ritardo.

La notifica all'Autorità di controllo deve contenere almeno: la descrizione della **natura della violazione** dei dati personali compresi, ove possibile, delle **categorie** e del **numero** approssimativo di **interessati** in questione nonché delle categorie e del numero approssimativo di **registrazioni** dei dati personali in questione; la comunicazione del **nome** e dei **dati di contatto** del responsabile della protezione dei dati (**DPO**) o di altro punto di contatto presso cui ottenere più informazioni; la descrizione delle probabili **conseguenze** della violazione dei dati personali; la descrizione delle **misure adottate** o di cui **si propone l'adozione** da parte del titolare del trattamento **per porre rimedio** alla violazione dei dati personali e anche, se del caso, per **attenuarne i possibili effetti negativi**.

In caso di violazione di dati personali, il titolare non è tenuto solamente alla notifica verso

l'Autorità di controllo, ma deve altresì **comunicare tale violazione agli interessati**, ovverosia a tutti i soggetti ai quali i dati oggetto della violazione si riferiscono.

La comunicazione del "*data breach*" verso gli interessati, deve essere effettuata negli stessi termini della notifica all'Autorità di controllo e deve contenere almeno: il **nome** e dei **dati di contatto** del responsabile della protezione dei dati (**DPO**) o di altro punto di contatto presso cui ottenere più informazioni; la descrizione delle probabili **conseguenze** della violazione dei dati personali; la descrizione delle **misure adottate** o di cui **si propone l'adozione** da parte del titolare del trattamento **per porre rimedio** alla violazione dei dati personali e anche, se del caso, per **attenuarne i possibili effetti negativi**.

Tuttavia, la comunicazione all'interessato non è richiesta quando i dati oggetto della violazione erano sottoposti a misure tecniche e organizzative tali da renderli incomprensibili a chiunque, quando il titolare ha tempestivamente introdotto misure tali da evitare rischi elevati sui dati personali e, infine, se la comunicazione richiede uno forzo sproporzionato (in tal caso si procede ad una comunicazione in forma pubblica).

Responsabilità e sanzioni

Riferimenti: artt. 82, 83, 84 RGDP

Com'è noto, rispetto al passato, una delle più rilevanti novità del Regolamento (UE) 2016/679 è rappresentata dall'elevato **inasprimento delle sanzioni amministrative pecuniarie**.

Le sanzioni amministrative pecuniarie previste dal Regolamento si articolano in due grandi scaglioni: le meno severe possono arrivare fino a **dieci milioni di euro**, o per le imprese fino al **2% del fatturato mondiale annuo se superiore**, mentre le più severe fino a **venti milioni di euro**, o per le imprese fino al **4%** del fatturato mondiale annuo.

La competenza ad infliggere le sanzioni amministrative è attribuita alle Autorità di controllo nell'ambito del territorio del rispettivo Stato membro. Per stabilire l'ammontare delle sanzioni devono essere valutati una serie di parametri, tra i quali: la **natura**, la **gravità** e la **durata della** violazione; il carattere **doloso** o **colposo** della violazione; le **misure adottate** dal titolare o dal responsabile del trattamento **per attenuare il danno** subito dagli interessati; il **grado di responsabilità** del titolare o del responsabile del trattamento tenendo conto delle **misure tecniche e organizzative** da essi messe in atto; eventuali **precedenti violazioni** pertinenti; il **grado di cooperazione** con l'autorità di controllo; le **categorie di dati personali** interessate dalla violazione.

Nell'ambito dei propri poteri correttivi, oltre a quello di irrogare sanzioni amministrative, dinnanzi ad una violazione delle norme previste dal Regolamento, le Autorità di controllo possono: rivolgere **avvertimenti** e **ammonimenti** al titolare o al responsabile del trattamento, **ingiungere** di **soddisfare le richieste dell'interessato** o di **conformare i trattamenti** alle disposizioni del regolamento, **imporre** una **limitazione provvisoria o definitiva al trattamento**, incluso il divieto di trattamento, **ordinare la rettifica**, la **cancellazione** di dati personali o la **limitazione del trattamento**,

revocare la certificazione e **ordinare la sospensione dei flussi di dati** verso l'estero.

Le conseguenze derivanti da un illecito trattamento di dati personali non si limitano esclusivamente ad una responsabilità di natura amministrativa, ma possono comportare altresì l'insorgere di una responsabilità sia di tipo civile che penale. Per quanto riguarda la responsabilità civile, questa consiste nel diritto dell'interessato di ottenere, in presenza di determinate condizioni, il risarcimento del danno cagionato dalla condotta dell'autore della violazione (in genere, il titolare o il responsabile del trattamento); per la responsabilità penale, invece, si applicano i principi e le norme di diritto penale vigenti in ciascuno Stato membro.